

DEPARTMENT OF THE NAVY  
Office of the Secretary  
Washington, DC 20350-1000

SECNAVINST 5510.31B  
NIPO-10  
31 December 1992

SECNAV INSTRUCTION 5510.31B

**From:** Secretary of the Navy  
**To:** All Ships and Stations

**Subj:** POLICY AND PROCEDURES FOR  
CONTROL OF FOREIGN DISCLOSURE  
IN THE DEPARTMENT OF THE  
NAVY

**Ref:** (a) NDP-1, National Policy and  
Procedures for the Disclosure of  
Classified Military Information to  
Foreign Governments and  
International Organizations  
(NOTAL)

**Encl:** (1) DOD Directive 5230.11 of 16 Jun  
92, Disclosure of Classified  
Military Information to Foreign  
Governments and International  
Organizations  
(2) DOD Directive 5230.20 of 24 Apr  
92, Visits and Assignments of  
Foreign Representatives

**1. Purpose.** To designate authority and responsibility for control of foreign disclosure in the Department of the Navy. This instruction is a substantial revision and should be reviewed in its entirety.

**2. Cancellation.** SECNAVINST 5510.31A.

**3. Background.** National Security Decision Memorandum (NSDM)-119 established National Disclosure Policy. Responsibility for implementation was delegated to the Secretary of Defense. Reference (a) issued national disclosure policy and procedures. Enclosure (1) delegated responsibility to the Secretary of the Navy (SECNAV) for national disclosure policy in the Department of the Navy (DON) and directed designation of a principal authority to control DON foreign disclosure and implement disclosure policies within DON. Enclosure (2) directs implementation of the DOD International Visitors Program (IVP) and Defense Personnel Exchange Programs (DPEP) within DON.

**4. Action.** The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RDA)) is designated principal disclosure authority within DON. Subject to overall responsibility of ASN (RDA) and oversight by the Deputy Assistant Secretary of the Navy for International Policy (DASN(IP)), Director, Navy International Programs Office (Navy IPO) is delegated authority to disclose or deny DON classified military information within the limitations of reference (a), provide DON representation to the National Disclosure Policy Committee (NDPC), and further delegate foreign disclosure authority in accordance with enclosure (1). Director, Navy IPO, will ensure implementation of enclosures (1) and (2) within DON and issue internal guidance and procedural instructions necessary for uniform application of disclosure controls.

**5. Report.** The reporting requirement contained in enclosure (1) is exempt from reports control by SECNAVINST 5214.2B.

DAN HOWARD  
Secretary of the Navy (Acting)

**Distribution:**

SNDL Parts 1 and 2

Headquarters Marine Corps (C41)

Washington, DC 20380-1775 (1 copy)

MARCORPS Codes PCN 71000000000 and  
71000000100

NAVY IPO-10

Washington DC 20350-5000 (100 copies)

SECNAV/OPNAV Directives Control Office

901 M Street SE Building 200

Washington DC 20374-5074 (30 copies)

**Stocked:**

Naval Aviation Supply Office

Physical Distribution Division Code 103

5801 Tabor Avenue

Philadelphia PA 19120-5099 (500 copies)

0579L00561480





Department of Defense  
**DIRECTIVE**

SECNAVINST 5510.31B

31 DEC 1992

June 16, 1992  
NUMBER 5230.11

USD(P)

**SUBJECT:** Disclosure of Classified Military Information to Foreign Governments and International Organizations

- References:**
- (a) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984 (hereby canceled)
  - (b) DoD Instruction 5230.17, "Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations," February 17, 1985 (hereby canceled)
  - (c) National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (short title: National Disclosure Policy (NDP-1)), October 1, 1988<sup>1</sup>
  - (d) through (t), see enclosure 1

**A. REISSUANCE AND PURPOSE**

This Directive reissues reference (a), replaces reference (b), implements reference (c), and updates policy, responsibilities, and procedures governing proposed disclosures of classified military information to foreign governments and international organizations (hereafter referred to as "foreign governments").

**B. APPLICABILITY AND SCOPE**

This Directive applies to:

1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").
2. All disclosures of classified military information defined in enclosure 2. Disclosures of military intelligence information, however, also must be in compliance with DoD Directive C-5230.23 (reference (d)).

---

<sup>1</sup> Provided to designated disclosure authorities on a need-to-know basis from the Office of the Director for International Security Programs, Office of the Deputy Under Secretary of Defense for Security Policy (ODUSD(SP)).

Enclosure (1)

3. Classified information involved in munitions license applications processed under DoD Directive 2040.2 and the ITAR (references (e) and (f)).

#### **C. DEFINITIONS**

Terms used in this Directive are defined in enclosure 2.

#### **D. POLICY**

It is U.S. national and DoD policy under NDP-1 (reference (c)) that:

1. Classified military information is a national security asset that shall be protected and shall be shared with foreign governments only when there is a clearly defined benefit to the United States. Disclosures of such information shall be made only when authorized by officials designated under this Directive and then only when all requirements of this Directive are met.

2. An official who has been specifically delegated disclosure authority under section E., below, may authorize disclosures of classified military information to foreign governments in support of a lawful and authorized U.S. Government purpose if the:

- a. Official represents the DoD Component that originated the information.
- b. Level of classified information to be disclosed does not exceed the classification level delegated by Annex A of reference (c).
- c. Criteria and conditions in enclosure 3 are satisfied.

3. The Secretary of Defense and the Deputy Secretary of Defense are the only DoD officials who have original authority to grant exceptions to the policy contained in this Directive. The Secretary of Defense has delegated authority to the National Military Information Disclosure Policy Committee (NDPC) to consider and grant requests for exceptions to policy in compliance with reference (c).

4. Classified military information shall not be disclosed to foreign nationals until the appropriate designated disclosure authority receives a security assurance from the recipient foreign government on the individuals who are to receive the information.

5. In accordance with reference (c), it is U.S. policy to avoid creating false impressions of U.S. readiness to make available classified military information, materiel, or technology. Accordingly, designated disclosure authorities of the originating DoD Component, or, when an exception to policy is required, the Secretary of Defense, the Deputy Secretary of Defense or the NDPC must authorize, in advance, proposals to be made to foreign governments that could lead to the eventual disclosure of classified

military materiel, technology, or information. Commitments shall not be expressed or implied, and no disclosures shall be made pending the required disclosure decision.

6. Disclosure planning shall include the following:

a. Planning for possible foreign involvement should start at the beginning of the weapon system acquisition process and other programs, to facilitate decisions on the disclosure of classified and controlled unclassified information in support of cooperative programs, foreign participation in the DoD procurement activities, and foreign sales. The planning shall include consideration of the requirements set forth in DoD Instruction 5000.2, Part 5, Section F (reference (g)).

b. The DoD Components shall use the Technology Assessment/Control Plan in DoD Directive 5530.3 (reference (h)) as the basis for making the stated disclosure decisions in paragraph D.6.a., above, on weapon system programs.

c. A delegation of disclosure authority letter (DDL) similar to that in enclosure 4 shall be used to provide disclosure guidance to subordinate commands and Agencies and, when applicable, to the DoD contractors.

7. All disclosures and denials of classified military information shall be reported in the Foreign Disclosure and Technical Information System (FORDTIS), in accordance with DoD Instruction 5230.18 (reference (i)). For denials, disclosure authorities must take special care to record a concise summary of the analysis that led to the denial.

8. Under conditions of actual or imminent hostilities, any Unified or Specified Commander may disclose classified military information through TOP SECRET to an actively participating allied force when support of combined combat operations requires the disclosure of that information. The appropriate U.S. Commander shall notify the Chairman of the Joint Chiefs of Staff of such disclosures. The Chairman of the Joint Chiefs of Staff, in turn, shall notify the Office of the Under Secretary of Defense for Policy, ATTN: Chairman, NDPC, who shall determine any limitations that should be imposed on continuing disclosure of the information. The U.S. Commander shall be informed of any limitations through the Chairman of the Joint Chiefs of Staff.

9. The classified military information that is approved for foreign disclosure shall be transmitted to the intended foreign recipient through government-to-government channels, in accordance with DoD 5200.1-R, chapter 8 (reference (j)).

E. RESPONSIBILITIES

1. The Under Secretary of Defense for Policy shall:

a. Ensure effective implementation of the National Disclosure Policy and operation of the NDPC under NDP-1 (reference (c)).

b. Designate the Chair of the NDPC, who shall represent the Secretary of Defense on the NDPC.

c. Advise the DoD Components and the NDPC about security matters on disclosures.

d. Draft and negotiate with foreign governments, in coordination with the other applicable DoD Components and Federal Departments and Agencies, security agreements governing the safeguarding of classified military information and equipment.

e. Coordinate on all international agreements negotiated under DoD Directive 5530.3 (reference (h)) that involve the disclosure of classified military information.

f. Review and approve, when justified, requests for disclosure authority from heads of the OSD organizational elements and the DoD Components not covered in subsection E.2., below.

g. Issue policy governing international visits, the assignment of liaison officers and exchange officers, and other assignments of foreign representatives to the DoD Components and defense contractors.

h. Maintain effective liaison with security officials of allied and friendly governments with which the U.S. Government has entered into security agreements.

i. Direct, manage, and control the FORDTIS, in accordance with DoD Instruction 5230.18 (reference (i)).

j. Issue necessary supplemental publications for the effective implementation of this Directive.

k. Publish an annual schedule to keep the DoD Components informed of security survey support requirements.

l. Record decisions rendered on requests for exception to reference (c) in the FORDTIS, in accordance with reference (i).

2. The Under Secretary of Defense for Policy, in addition to the responsibilities in subsection E.1., above, and the Secretaries of the Military Departments, the Under Secretary of Defense (Acquisition), the Chairman of the Joint Chiefs of Staff, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), the Director, Defense Intelligence Agency, and the Director, National Security Agency/Central Security Service, shall:

a. Authorize disclosures or denials of the U.S. classified military information for which they are the originating DoD Component in accordance with this Directive.

b. Designate a senior official to be the principal disclosure authority for their DoD Component. Such designations shall be in writing, with a copy provided to the Chair of the NDPC.

c. Provide disclosure authority, in writing, to the heads of commands and Agencies and major staff elements under their direction, control, or authority, as necessary, to ensure efficient operation of those commands, Agencies, and staff elements.

d. Require that the heads of commands, Agencies, and staff elements to whom disclosure authority has been provided appoint a designated disclosure authority.

e. Coordinate with the Chair of the NDPC all proposed disclosure decisions to be referred directly to the Secretary of Defense or the Deputy Secretary of Defense.

f. Provide the necessary support to the Chair of the NDPC to do security surveys of foreign government security programs. (See subparagraph F.9.c.(2), below.)

g. Forward any inquiries concerning this Directive to the Office of the Under Secretary of Defense for Policy, Attn: Deputy Under Secretary of Defense (Security Policy).

h. Ensure that the principal disclosure authorities shall:

(1) Control disclosures for their respective DoD Component.

(2) Ensure the competency of subordinate officials appointed as designated disclosure authorities.

(3) Ensure that all proposed disclosure actions originating in their DoD Component are coordinated with the other DoD Components that have a joint or shared interest in the information involved.

(4) Designate a member and an alternate to represent their DoD Component on the NDPC and ensure that the persons designated:

(a) Are thoroughly familiar with the daily administration of disclosure activities in their respective DoD Component.

(b) Are qualified to provide broad professional guidance on matters brought before the NDPC.

(c) Have direct access to the DoD Component's principal disclosure authority as well as to other members of the NDPC.

(5) Ensure that their DoD Component's disclosure decisions are reported to the FORDTIS in accordance with DoD Instruction 5230.18 (reference (i)).

(6) Coordinate requests for disclosures of classified military information involved in litigation with the General Counsel of the Department of Defense or the General Counsel of the DoD Component concerned, as appropriate, before determining whether to disclose the requested information.

(7) Ensure that Component personnel traveling overseas are provided disclosure guidance and are informed of and comply with the policy for overseas travel described in DoD 5200.1-R, chapter 8 (reference (j)).

3. The Chairman of the Joint Chiefs of Staff shall represent the Commanders of the Unified and Specified Commands on the NDPC.

4. The General Counsel of the Department of Defense shall:

a. Ensure the legal adequacy of security agreements between the United States and foreign governments that establish procedures for the protection of the classified military information.

b. Advise the DoD Components and the NDPC on the legal aspects of applying the NDP-1 (reference (c)) to individual disclosure decisions.

5. The Assistant to the Secretary of Defense (Atomic Energy) shall inform the other NDPC members on the current implementation of international agreements made under the Atomic Energy Act (reference (k)). That includes any statutory determinations and requirements placed on recipient foreign governments and international organizations for safeguarding atomic information released to them.

6. The Secretary of the Air Force shall provide resources for the operation, maintenance, and administration of the FORDTIS, and comply with DoD 7110.1-M (reference (l)) on requests for funds to carry out that FORDTIS responsibility.

## F. PROCEDURES

### 1. International Agreements

a. Early Disclosure Determination. Before any discussions with foreign representatives on the negotiation of an international agreement that is governed by DoD Directive 5530.3 (reference (h)), the DoD Components shall determine the extent to which classified military information will be required for release, and obtain disclosure authorization for the information. (See subsection D.6., above.)

b. Security Requirements. International agreements that involve the disclosure of classified military information shall contain, at a minimum, the security requirements in section B. of enclosure 3. If a general security agreement exists with the foreign government concerned, this requirement may be satisfied by referencing that agreement.

Such agreements shall be coordinated with the Office of the Under Secretary of Defense for Policy, ATTN: Deputy Under Secretary of Defense (Security Policy), who may specify other requirements during coordination.

c. Cooperative Programs. Disclosure authorities shall review carefully any request for classified military information made in accordance with a cooperative agreement with both the goals of the program and the interests of national security in mind.

2. Meetings, Symposia, and Conferences. The conduct and organization of meetings, symposia, and conferences where classified military information is to be disclosed shall be in accordance with DoD Directive 5200.12 and DoD 5200.1-R (references (m) and (j)).

a. Foreign Participation. Foreign nationals may participate in such gatherings when their participation is in accordance with this Directive and U.S. export control policies, the appropriate designated disclosure authorities have approved any classified or controlled unclassified information for disclosure to the proposed foreign attendees, the foreign attendees actively participate in the proceedings, and there is reciprocity for the U.S. Government and industry representatives.

b. Disclosure Levels. The classification levels and categories of information authorized for disclosure vary among nations. The DoD Components shall limit the level of classified information to be disclosed at meetings attended by foreign representatives to the lowest level that is common to all nations represented.

3. Foreign Visitors, Liaison Officers, and Exchange Personnel. Procedures on such individuals shall be in accordance with DoD Directive 5230.20 (reference (n)). Disclosures of classified information shall be in accordance with this Directive.

4. Sales, Leases, Loans, or Grants of Classified Items. In implementing the policy in subsection D.5., above, the DoD Components shall comply with the following standards when authorizing the disclosure or commercial export of any information, classified or unclassified, relating to sales, leases, loans, or grants of military equipment:

a. Release Authorization. Before approval of initiatives that could lead to a sale, lease, loan, or grant of military equipment, obtain authorization from the appropriate designated disclosure authority for disclosure of all necessary classified equipment and information required for system operation, employment, maintenance, and training, including system software.

b. Initial Disclosures. Limit initial disclosures to general information, usually no higher than CONFIDENTIAL, on system characteristics, capabilities, and price and availability until a sale, lease, loan, or grant is consummated.



c. System Countermeasures. Withhold specific information on system countermeasures susceptibilities or vulnerabilities and counter-countermeasures capabilities, until the sale, lease, loan, or grant is consummated.

d. Operation, Employment, Maintenance, and Training. After consummation of a sale, lease, loan, or grant, classified military information may be disclosed up to the level necessary for operation, employment, maintenance, and training.

e. Data Packages. Edit or rewrite data packages to exclude information that is beyond that which has been authorized for disclosure.

(1) The disclosure of technical data for production purposes shall be limited to data that is necessary to produce a specific item that is approved for release to the country that is to receive the data.

(2) The disclosure of technical data for maintenance purposes shall be limited to data that is necessary to perform the level of maintenance that has been authorized for the country that is to receive the data.

## 5. Foreign Test and Evaluation

a. Foreign test and evaluation of the U.S. classified equipment may be authorized when the tests:

(1) Are on an item approved for foreign disclosure by the appropriate disclosure authority.

(2) Can be performed at a U.S. installation or under other strict U.S. control that guarantees appropriate safeguards for classified information and classified or unclassified critical technology.

b. Exceptions to subparagraph F.5.a.(2), above, such as the transfer of a single classified military item for test and evaluation under foreign security control, may be authorized only when all of the following conditions are fulfilled:

(1) There is no transfer of, and the test will not reveal, technology that the United States would not license for manufacture in the foreign country.

(2) There is no release of equipment that would not be approved for foreign sale or export to the foreign country, if requested.

(3) The release will result in a clearly defined advantage to the United States; for example:

(a) Specifically defined avoidance of significant costs or acceleration of programs in development efforts by the United States and its allies.

(b) Advance the objectives of standardization with and among U.S. allies by promoting cooperation in research and development.

(c) Exchange technical and scientific information of common interest on a mutually beneficial basis.

(4) The Secretary of the Military Department concerned, in coordination with the Office of the Under Secretary of Defense (Acquisition), approves the exception as meeting the described conditions in paragraph F.5.b., above. The Chair of the NDPC shall be informed of each exception; the Chair shall notify the NDPC members.

(5) The test is performed under a test and evaluation agreement negotiated under DoD Directive 5530.3 (reference (h)), or a lease arrangement or sales contract containing requisite security controls.

(6) The releases are reported to the FORDTIS.

#### 6. Foreign Participation in DoD Component Classified Training Activities

a. Receiving Training on U.S. Equipment. A foreign national may receive training on U.S. equipment that is classified or involves classified information, if the equipment is in the inventory of or is to be acquired by the trainee's government after the following:

(1) The prospective trainee's government has concluded an international agreement or signed a purchase agreement with the United States to acquire the equipment and training; or

(2) The Defense Security Assistance Agency has issued an International Military Education and Training (IMET) order for the training.

b. Conducting Training on U.S. Equipment. A foreign national may conduct training on U.S. equipment that is classified or involves classified information, if the item has been sold or otherwise provided to the foreign national's government and the U.S. Government has specifically approved the provisions of such training to any third party that is involved.

c. Third-Country Equipment. Foreign nationals may receive or conduct training on equipment provided by a third-country that is classified or involves third-country classified information only with the prior written consent of the government that provided the equipment.

#### 7. Requests for Classified Documents

a. Disclosure Review. Requests for classified documents by a foreign representative shall be forwarded to the applicable designated disclosure authority of the

originating DoD Component for review and approval or denial. The requests shall be processed using the FORDTIS, when practicable.

b. Report to the FORDTIS. The designated disclosure authority that renders the decision shall report it to the FORDTIS under DoD Instruction 5230.18 (reference (i)).

c. Reference Lists and Bibliographic Material. To avoid false impressions and to avoid proliferation of requests for classified military information that is not releasable to the requestor, the DoD Components shall:

(1) When practical, excise references to nonreleasable documents and information from material that may be otherwise released.

(2) Discourage release of documents that are reference lists or are bibliographic. To react favorably to justified foreign requests for information, identify the requestor's specific requirements and provide only the U.S. information that satisfies that requirement and is determined to be releasable.

8. Foreign Access to Information When Participating in U.S. Procurement Programs. Participation consistent with applicable U.S. laws, regulations, and security requirements in DoD procurement initiatives by contractors from countries with which the Department of Defense has agreements that encourage reciprocal participation in defense procurement may include access to classified information consistent with this Directive as follows:

a. Access to Technical Data. Qualified government and industry representatives from those countries shall be given appropriate access to technical data, consistent with this Directive and the ITAR (reference (f)), necessary to bid on the DoD contracts.

b. Disclosure Decisions. Disclosure decisions involving those countries shall be made before the announcement of the procurement (see subsection D.6., above), and the announcement shall describe any restrictions on foreign participation.

c. Participation as Subcontractor. When it is determined that foreign contractors are not authorized to participate in the classified or other sensitive aspects of a potential contract, consideration should be given to their requests for participation in unclassified or less sensitive aspects of the contract as a subcontractor.

d. Requests for Documentation. Requests by foreign entities for classified or controlled unclassified documentation must be submitted through government channels.

9. NDPC Operations. The following procedures apply to the activities below:

a. Exceptions to NDP-1

(1) Exceptions to NDP-1 (reference (c)), other than those granted by the Secretary of Defense or the Deputy Secretary of Defense, shall be granted only by the NDPC.

(2) All proposed disclosure actions that require decisions by the Secretary of Defense or the Deputy Secretary of Defense shall contain the views of the originating DoD Component or Agency and shall be coordinated with the Chair of the NDPC.

(3) When the Secretary of Defense or the Deputy Secretary of Defense grants an exception to policy, the DoD Component originating or participating in the determination shall notify the Chair of the NDPC so that the exception may be recorded properly and reported promptly to the NDPC members and the National Security Council and recorded in the FORDTIS.

(4) All other requests for exception to policy shall:

(a) Be forwarded through channels to the designated disclosure authority who represents the requestor's organization on the NDPC.

(b) At a minimum, include the information in enclosure 5.

b. Reporting to the NDPC of Compromises of U.S. Classified Military Information Furnished to Foreign Governments. The DoD Components having knowledge of compromises of U.S. classified information by foreign governments promptly shall inform the originating DoD Component. The originating DoD Component shall conduct a damage assessment and shall provide copies of the completed case report and damage assessment to the Chair of the NDPC. If the originating DoD Component is not known, the Chair of the NDPC shall conduct the damage assessment and prepare the case report. In either situation, the Chair of the NDPC shall provide the NDPC with an evaluation to serve as a basis for determining whether the nature of the compromise requires a change in reference (c).

c. Operation of the NDPC

(1) NDP-1, NDPC Record of Action 001.7/70 (references (c) and (o)), and this Directive govern the DoD Component participation in the NDPC operations.

(2) The DoD Components shall provide qualified personnel to participate on the NDPC security survey teams, when requested. The parent DoD Component shall bear travel and per diem expenses for participants.

(3) The DoD members of NDPC security survey teams shall participate in pre-departure briefings, all scheduled team activities, and the preparation of all reports and briefings resulting from the security survey.

d. Cooperation with the NDPC. Under the NDP-1 (reference (c)), the Chair of the NDPC acts for and in the name of the Secretary of Defense in carrying out the decisions of the NDPC. All of the DoD Components shall support the Chair's requests for assistance in disclosure matters.

10. Classification Requirements. DoD 5200.1-R (reference (j)) governs classification and safeguarding of classified information. The DoD Components also shall follow the security classification guide for NDP matters in enclosure 6.

#### G. INFORMATION REQUIREMENTS

The reports referenced in this Directive are exempt from licensing in accordance with paragraph E.4.b. of DoD 7750.5-M (reference (p)).

#### H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Under Secretary of Defense for Policy within 120 days.



Donald J. Atwood  
Deputy Secretary of Defense

#### Enclosures - 6

1. References
2. Definitions
3. NDP-1 Disclosure Criteria, Conditions, and Limitations
4. The DDL
5. Requests for Exception to Policy
6. Security Classification Guide for NDP

REFERENCES, continued

- (d) DoD Directive C-5230.23, "Intelligence Disclosure Policy. (U)," November 18, 1983
- (e) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984
- (f) Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulations (ITAR)"
- (g) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991
- (h) DoD Directive 5530.3, "International Agreements," June 11, 1987
- (i) DoD Instruction 5230.18, "The DoD Foreign Disclosure and Technical Information System (FORDTIS)," November 6, 1984
- (j) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
- (k) Public Law 83-703, "Atomic Energy Act of 1954," August 30, 1954, as amended (Sections 2121, 2153, and 2164 of title 42, United States Code)
- (l) DoD 7110.1-M, "Department of Defense Budget Guidance Manual," May 1990, authorized by DoD Instruction 7110.1, October 30, 1980
- (m) DoD Directive 5200.12, "Conduct of Classified Meetings," May 16, 1988
- (n) DoD Directive 5230.20, "Control of Foreign Representatives," June 25, 1984
- (o) National Military Information Disclosure Policy Committee Record of Action 001.7/70, "NDPC Detailed Operating Procedures," September 15, 1981
- (p) DoD 7750.5-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 7750.5, August 7, 1986
- (q) Executive Order 12356, "National Security Information," April 2, 1982
- (r) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
- (s) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
- (t) Title 15, Code of Federal Regulations, Parts 730-799, "Export Administration Regulations (EAR)"

## **DEFINITIONS**

1. **Classified Military Equipment.** Military equipment that is itself classified; contains classified information that may be derived from or revealed by its operation or testing; or will require the disclosure of classified information for operation, employment, maintenance, or training.
2. **Classified Military Information.** Information originated by or for the Department of Defense or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL, as described in E.O. 12356 (reference (q)). Classified military information may be in oral, visual, or material form and has been subdivided further into the eight categories described below:
  - a. **Category 1 - Organization, Training, and Employment of Military Forces**  
Information of a general nature pertaining to tactics, techniques, tactical doctrine, and intelligence and counterintelligence doctrine and techniques. Excluded is information necessary for the operation, training, and maintenance on specific equipment covered under Categories 2 and 3, below.
  - b. **Category 2 - Military Materiel and Munitions.** Information on specific items of equipment already in production, or in service, and the information necessary for the operation, maintenance, and training. Items on the U.S. Munitions List fall within this category. This category does not pertain to equipment that is in research and development.
  - c. **Category 3 - Applied Research and Development Information and Materiel**  
Information related to fundamental theories, design, and experimental investigation into possible military applications; it includes engineering data, operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when the equipment has completed suitability testing and has been adopted for use or production.
  - d. **Category 4 - Production Information.** Information related to designs, specifications, manufacturing techniques, and such related information necessary to manufacture materiel and munitions.
  - e. **Category 5 - Combined Military Operations, Planning, and Readiness**  
Information necessary to plan, ensure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. It does not include strategic plans and guidance or North American defense information.

f. Category 6 - U.S. Order of Battle. Information pertaining to U.S. forces in a specific area. In general, disclosures of this information are limited to those countries in which U.S. forces are stationed or are in adjacent geographical areas.

g. Category 7 - North American Defense. Information related to plans, operations, programs, and projects, to include data and equipment, directly related to North American defense.

h. Category 8 - Military Intelligence. Information of a military character pertaining to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the Director of Central Intelligence (DCI).

3. Controlled Unclassified Information. Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes U.S. information that is determined to be exempt from public disclosure in accordance with DoD Directives 5230.25 and 5400.7 (references (r) and (s)) or that is subject to export controls in accordance with the ITAR (reference (f)) or the EAR (reference (t)).

4. Delegation of Disclosure Authority Letter (DDL). A letter issued by the appropriate designated disclosure authority explaining classification levels, categories, scope, and limitations of information under a DoD Component's disclosure jurisdiction that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate disclosure authorities.

5. Designated Disclosure Authority. An official, at subordinate component level, designated by the Head of a DoD Component or the Component's Principal Disclosure Authority to control disclosures of classified military information by his or her organization.

6. Disclosure. Conveying classified information, in any manner, to an authorized representative of a foreign government.

7. Foreign Disclosure and Technical Information System (FORDTIS). An automated system to assist decision makers and analysts in reviewing, coordinating, and reaching decisions concerning proposals to release classified military information, materiel, and technology to foreign governments.

8. Government-to-Government Channels. The principle that classified information and materiel will be transferred by government officials through official channels or through other channels expressly agreed upon by the governments involved. In either case, the information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.



9. Intelligence. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.
10. International Organization. An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.
11. Joint Information. Military information over which two or more DoD Components, or two or more Federal Departments or Agencies, exercise control, jurisdiction, or security awareness.
12. Meeting. A conference, seminar, symposium, exhibit, convention, training course, or other gathering during which classified or controlled unclassified information is disclosed.
13. Originating DoD Component. The DoD Agency that exercises original classification jurisdiction for classified information.
14. Security Assurance. The written confirmation, requested by and exchanged between governments, of the security clearance level or eligibility for clearance, of their employees, contractors, and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of U.S. classified military information possesses the requisite security clearance and is approved by his or her government for access to information of the security classification involved on behalf of the foreign government and that the recipient will comply with any security requirements specified by the United States. In the case of industrial facilities, the security assurance should include a statement concerning the level of storage capability.
15. Sensitive Compartmented Information. Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.
16. Strategic War Plan. A plan for the overall conduct of a war.

## **NDP-1 DISCLOSURE CRITERIA, CONDITIONS, AND LIMITATIONS**

A. **Disclosure Criteria.** Disclosures of classified military information in Categories 1 through 8 defined in item 2 of enclosure 2 may be made only when all of the criteria listed in subsections A.1. through 5., below, are satisfied. Disclosures in Category 8 also must be in compliance with DoD Directive C-5230.23 (reference (d)).

1. Disclosure is consistent with U.S. foreign policy and national security objectives concerning the proposed recipient foreign government. For example:

- a. The recipient government cooperates with the United States in pursuance of military and political objectives that are compatible with those of the United States.
- b. A specific U.S. national purpose, diplomatic or military, will be served.
- c. The information will be used in support of mutual defense and security objectives.

2. Disclosure is consistent with U.S. military and security objectives. For example:

- a. Disclosures of advanced technology, if compromised, will not constitute an unreasonable risk to the U.S. position in military technology and operational capabilities, regardless of the intended recipient.
- b. The proposed disclosure reflects the need for striking a proper balance between pursuit of our mutual defense and foreign policy objectives on the one hand and the preservation of the security of our military secrets on the other.

3. The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the United States. (The intent of a foreign government to protect U.S. classified military information is established in part by the negotiation of a General Security of Information Agreement or other similar security arrangement. A foreign government's capability to protect U.S. classified military information normally is determined by the evaluation of embassy security assessments, Central Intelligence Agency risk assessments, National Military Information Disclosure Policy Committee (NDPC) Security Survey Reports, and/or historical precedence.)

4. Disclosures will result in benefits to the United States at least equivalent to the value of the information disclosed. For example:

- a. The United States obtains information from the recipient nation on a quid pro quo basis.

b. The exchange of military information or participation in a cooperative project will be advantageous to the United States from a technical or other military viewpoint.

c. The development or maintenance of a high level of military strength and effectiveness on the part of the government receiving the information will be advantageous to the United States.

5. The disclosure is limited to information necessary to the purpose for which disclosure is made. For example, if the purpose of the disclosure is the sale of military equipment, information on operation, maintenance, and training would be released. Research and development data, or production know-how, must be withheld.

**B. Disclosure Conditions.** After a decision is made to disclose classified military information to a foreign government or international organization, based on the criteria listed in subsections A.1. through 5. of this enclosure, above, or an exception to policy, release of the classified military information will be contingent upon agreement by the recipient foreign government that the listed minimal conditions in subsections B.1 through 8., below, will be met. The conditions normally are satisfied by the provisions of existing General Security of Information Agreements. When a General Security of Information Agreement does not exist, the conditions may be included in a program-specific agreement, government contract, or similar arrangement.

1. The information or acknowledgment of its possession will not be revealed to a third-country government, organization, or person, except with the prior written permission of the originating U.S. Department or Agency.

2. The information will be afforded substantially the same degree of security protection afforded to it by the United States.

3. The information will be used only for designated military purposes, or other specified purposes.

4. The recipient will report promptly and fully to U.S. authorities any known or suspected compromise of U.S. classified military information released to it.

5. All individuals and facilities that will have access to the classified military information and materiel will have security clearances granted by their government at a level equal to that of the classified information involved and an official need-to-know.

6. The information will be transferred through government-to-government channels.

7. Security experts of each government will be permitted to visit the other government, when mutually convenient, to review and discuss each other's policies and practices for protecting classified information.

8. The recipient of the information agrees to abide by or meet U.S.-specified special terms and conditions for the release of U.S. information or materiel.

C. Disclosure Limitations

1. General Limitations. Nothing in this Directive shall be construed so as to allow the disclosure of the following types of information:

a. Prohibited by Law or Agreement. Classified information, the disclosure of which is prohibited by Federal law or by any international agreement to which the United States is a party.

b. Naval Nuclear Information. Any naval nuclear propulsion information, classified or unclassified, except under an agreement negotiated pursuant to the Atomic Energy Act of 1954, as amended (reference (k)).

c. Proprietary Information. Classified or unclassified proprietary information, the rights to which are owned by private firms or citizens (i.e., patents, copyrights, or trade secrets) without the owner's consent, unless such disclosure is authorized by relevant legislation, and then release will be subject to such legislation.

d. National Intelligence. National Intelligence or interdepartmental intelligence produced within the National Foreign Intelligence Board (NFIB) structure. Such intelligence cannot be disclosed without authorization of the DCI in accordance with applicable policies.

e. National Security Telecommunications and Information Systems Security Information. The National Security Telecommunications and Information Systems Security Committee is authorized by its terms of reference to make disclosures of classified military telecommunications and information systems security equipment and information without reference to the NDPC.

f. Counterintelligence. Operational information related to counterintelligence activities and disclosures related thereto.

g. Atomic Information. Such disclosures are made in accordance with the Atomic Energy Act of 1954, as amended (reference (k)).

h. Strategic Planning and Guidance. Only the Secretary of Defense or the Deputy Secretary of Defense may authorize the disclosure of plans, concepts, or other

information about strategic war plans. Requests for such disclosure shall be submitted through the Chairman of the Joint Chiefs of Staff.

2. Specifically Prohibited Disclosures. The following types of classified information are specifically prohibited from disclosure:

a. Classified information officially obtained from a foreign government, except when the information has been conveyed by the government with express written consent to its further disclosure.

b. Combined information without prior agreement of all parties.

c. Joint information without prior agreement of all Departments or Agencies having control or jurisdiction.

d. Information originated by or for another Department or Agency, unless that Department or Agency consents to the disclosure.

e. Intelligence information described in section I, subparagraph 5.c.(2) and section II, subparagraph 5.b.(7) of NDP-1 (reference (c)).

## THE DDL

The following DDL format should be used by the DoD Components: (While all elements identified should be provided in the general order shown, information should be presented in the clearest and easiest-to-use manner. For example, the usefulness of the DDL for complex systems will be enhanced if items 5 and 6 are broken out by major subsystems and software and disclosures are discussed separately.)

TITLE:

DATE:

1. CLASSIFICATION: Identify highest classification of information to be disclosed.
2. DISCLOSURE METHODS: E.g., oral, visual, or documentary.
3. CATEGORIES PERMITTED: Specify National Disclosure Policy categories to be disclosed.
4. SCOPE: Specify who is authorized to release material or information, and to whom disclosure is authorized.
5. AUTHORIZED FOR RELEASE AND/OR DISCLOSURE: Describe materiel and/or information that can be released or disclosed.
6. NOT AUTHORIZED FOR RELEASE AND/OR DISCLOSURE: Describe materiel and/or information that cannot be released or disclosed. (In addition to providing specific descriptions of releasable and restricted materiel and information, items 5 and 6 will also specify any conditions or limitations to be imposed; e.g., time-phasing of release, allowable forms for software, identification of items releasable only as finished, tested assemblies, etc.)
7. PROCEDURES: Specify review and release procedures, special security procedures, or protective measures to be imposed.
8. REDELEGATION: Specify the extent of redelegation of authority (if any) permitted to subordinate activities.

## **REQUESTS FOR EXCEPTION TO POLICY**

Requests for an exception to policy shall contain the following elements of information:

1. A concise statement of the action proposed. Include security classification and categories of U.S. classified military information to be disclosed. (For example: "The OUSD(A) member, National Disclosure Policy Committee (NDPC), requests an exception to the National Disclosure Policy to permit the disclosure of SECRET Category 3 (Applied Research and Development Information and Materiel) information to the Government of \_\_\_\_\_ in support of the negotiation of a Data Exchange Agreement pertaining to surface-to-air missiles.")
2. A precise statement of why an exception to policy is required. (For example: An exception is required because (a) the level of classified information involved exceeds the classification level delegated in Annex A of NDP-1; or (b) the proposed action is not in consonance with policy currently established in Annex B or C of NDP-1; or (c) certain (identify which) of the disclosure criteria or conditions listed in section II. of NDP-1 are not fully met; or (d) any or all of the above in combination.)
3. An assessment of how each of the disclosure criteria and conditions in section II. of NDP-1 shall be met:
  - a. "Disclosure is consistent with the foreign policy of the United States toward the Government of \_\_\_\_\_." (A further detailed discussion shall be included to substantiate this statement. Reference shall be made to Presidential, National Security Council, or other high-level policy decisions to support the justification provided. A simple statement such as "the recipient cooperates with the United States in pursuance of military and political objectives" is not sufficient.)
  - b. "The military security of the United States permits disclosure." (If equipment or technology is involved, there must be a discussion on the result of a compromise on U.S. operational capability or the U.S. position in military technology. This discussion shall include an analysis of the state of the art regarding the technology involved, the susceptibility of the item to reverse engineering, the capability of the foreign recipient to reverse engineer the item, the foreign availability of the technology or equipment involved, and other governments to whom similar equipment or technology has been released.)
  - c. "The foreign recipient will afford the information substantially the same degree of security protection given to it by the United States." (If there has been an NDPC Security Survey for the proposed recipient, the conclusion reached therein shall be discussed. In the absence of an NDPC Security Survey, efforts shall be made to obtain, through intelligence channels, a counterintelligence risk assessment or security analysis of

the foreign government's security capabilities. The mere statement that "classified information has been released previously to this government and there is no indication that such information has been compromised" is not sufficient.)

d. "Disclosures will result in benefits to the United States at least equivalent to the value of the information disclosed." (For example: (1) if the United States obtains information from the proposed recipient on a quid-pro-quo basis, describe the information and the value to the United States; (2) explain how the exchange of military information for participation in a cooperative project will be advantageous to the United States from a technical or military capability viewpoint; (3) if the development or maintenance of a high degree of military strength and effectiveness on the part of the recipient government will be advantageous to the United States, explain how.)

e. "The disclosure is limited to information necessary to the purpose for which disclosure is made." (For example, if the purpose of the request is for the sale of equipment only, it shall be indicated clearly that research and development data or production know-how is not to be divulged or that documentation will be sanitized.)

4. Any limitations placed on the proposed disclosure in terms of information to be disclosed, disclosure schedules, or other pertinent caveats that may affect NDPC approval or denial of the request. (If disclosures are to be phased or if certain information is not to be released, the phasing or nonreleasable information shall be specified.)

5. A statement that the requested exception is to be either a continuing exception, subject to annual review, or a one-time exception. (A continuing exception usually is associated with a long-term project, such as a coproduction program or military sale when the United States will be obligated to provide life-cycle support. A one-time exception typically is used for a briefing or demonstration or short-term training.)

6. The names and titles of U.S. officials accredited to the requesting foreign government or international organization with whom the proposed exception has been coordinated, as well as the views of the Theater Commander. (Sufficient time shall be allowed to obtain an opinion from U.S. Embassy personnel in-country and the responsible Theater Commander before submitting the request for approval. Many cases are delayed because a U.S. Embassy or Theater Commander opinion has not been obtained.)

7. The opinion of other interested Departments or Agencies if joint Service or shared information is involved. (If the information or item of equipment is of shared or joint interest, such as an air-to-air missile used by two Services or containing technology of concern to another Service, the views of the other party will be included.)

8. Any information not mentioned above that would assist the NDPC members, the Secretary of Defense, or the Deputy Secretary of Defense in evaluating the proposal.



9. The name and telephone number of a knowledgeable individual within the requesting organization who can provide additional technical detail or clarification concerning the case at issue.

10. The date a response is desired on the case. Ten full working days for NDPC case deliberations should be allowed. The suspense date (10 full working days) is computed starting from the first full working day after the date of the request.

SECURITY CLASSIFICATION GUIDE FOR  
NATIONAL DISCLOSURE POLICY

<u>SUBJECT MATTER</u>	<u>CLASSIFICATION</u>	<u>REMARKS</u>
A. The Charts in Annex A of NDP-1 (reference (c)).	SECRET	
1. The association of a foreign country or international organization with one or more disclosure category entries quoted from the chart in Annex A of reference (c).	CONFIDENTIAL	
2. The association of one or more disclosure category entries in the charts in Annex A of reference (c) pertaining to two or more foreign countries or international organizations (that is, any comparison of the disclosure levels of two or more countries or international organizations).	SECRET	
B. The fact that a specific foreign country or international organization has agreed to afford U.S. classified military information the same degree of protection as afforded by the U.S. Government.	UNCLASSIFIED	Unless the mere existence of the governing security agreement is classified, in which case the same classification applies. This can be determined by reviewing Part B of the charts in Annex A of reference (c).
C. Disclosure authority as set forth in section II.4. of reference (c).	UNCLASSIFIED	
D. Disclosure criteria (and examples) set forth in section II.5.a. of reference (c) without reference to a specific case or country.	UNCLASSIFIED	

<u>SUBJECT MATTER</u>	<u>CLASSIFICATION</u>	<u>REMARKS</u>
E. Disclosure criteria for military intelligence as set forth in section II.5.b. of NDP-1 (reference (c)) and DoD Directive C-5230.23 (reference (d)).	CONFIDENTIAL	Unless otherwise specified by the paragraph markings in section II.5.b.
F. Disclosure conditions for classified military information as set forth in section II.6. of reference (c).	UNCLASSIFIED	
G. NDPC organization and membership in section III. of reference (c).	UNCLASSIFIED	
H. NDPC procedures enumerated in section IV. of reference (c).	UNCLASSIFIED	Except for section IV.2.b. which is CONFIDENTIAL.
I. Specific disclosure policy, in addition to that in the chart in Annex A of reference (c), relative to a specific country or international organization.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.
J. Specific disclosure policy for selected weapon systems, equipment, and technologies.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.
K. Information revealing the security policies, procedures, methods, or practices of a foreign country or international organization for protecting classified military information compiled by a NDPC Security Survey Team.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.

<u>SUBJECT MATTER</u>	<u>CLASSIFICATION</u>	<u>REMARKS</u>
L. Assessments, including deficiencies or recommendations, compiled by an NDPC Security Survey Team that would not result in adverse effects of foreign relations if disclosed but that could result in damage to the national defense if disclosed. For example, the deficiency concerns an exploitable vulnerability that, if revealed, could cause direct or immediate jeopardy to the security of U.S. classified information.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.
M. Deficiencies or recommendations compiled by the NDPC Security Survey Team that could result in adverse effects on foreign relations if disclosed.	CONFIDENTIAL	Other classification levels will be recommended to the Chairman of the NDPC when circumstances warrant.

6-3  
N. The above items shall be declassified on "OADR."



# Department of Defense DIRECTIVE

SECNAVINST 5510.31B

31 DEC 1992

April 24, 1992  
NUMBER 5230.20

USD(P)

**SUBJECT:** Visits and Assignments of Foreign Representatives

- References:**
- (a) DoD Instruction 5230.20, "Control of Foreign Representatives," June 25, 1984 (hereby canceled)
  - (b) Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulations (ITAR)"
  - (c) Title 15, Code of Federal Regulations, Parts 730-799, "Export Administration Regulations (EAR)"
  - (d) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," January 1991, authorized by DoD Directive 5220.22, December 8, 1980
  - (e) through (r), see enclosure 1

## **A. REISSUANCE AND PURPOSE**

This Directive:

1. Reissues reference (a) and updates policy and responsibilities governing visits by foreign representatives and the assignment of foreign nationals to the DoD Components.
2. Establishes the International Visits Program (IVP) and Defense Personnel Exchange Program (DPEP).

## **B. APPLICABILITY AND SCOPE**

This Directive:

1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").
2. Applies to all arrangements whereby foreign representatives visit or are assigned to the DoD Components or to facilities over which DoD Components have security responsibility.
3. Does not apply to visits conducted at DoD contractor facilities that involve access only to unclassified information that is not subject to export licensing under the Department of State's International Traffic in Arms Regulations (ITAR) (reference (b)) or the Department of Commerce's Export Administration Regulations (EAR) (reference (c)).

Enclosure (2)

4. Does not apply to visits to the DoD Components or DoD contractor facilities by foreign national employees of a U.S. contractor. Such visits will be processed in accordance with the ITAR, DoD 5220.22-M (references (b) and (d)), and subsection B.4. of enclosure 3.

### **C. DEFINITIONS**

Terms used in this Directive are defined in enclosure 2. (Only these terms will be used for IVP and DPEP visits and assignments.)

### **D. POLICY**

It is DoD policy that:

1. All visits and assignments of foreign representatives to the DoD Components that will involve access to classified or controlled unclassified information, or that will involve access to locations where access is controlled, shall be conducted under the IVP or the DPEP and in accordance with this Directive.

2. Visits by foreign representatives and assignments of liaison officers to the DoD Components shall be arranged under the procedures for a one-time visit, a recurring visit, or an extended visit as described in enclosure 3.

a. DoD visit authorizations shall not be used to circumvent export licensing requirements. (See subsection B.8. of enclosure 3.)

b. Visits shall be sponsored by the visitor's government. Requests for visits within the United States shall be submitted through the requesting government's Embassy in Washington, DC.

3. Assignments of foreign representatives to DoD Component organizations to perform functions for the host DoD organization shall be arranged only under a DPEP agreement concluded under DoD Directive 5530.3 (reference (e)) and enclosure 4.

4. Access by foreign representatives to classified information shall be in accordance with DoD Directive 5230.11 and DoD 5200.1-R (references (f) and (g)).

5. Access by foreign representatives to controlled unclassified information shall be in accordance with DoD Directives 5230.25 and 5400.7 (references (h) and (i)).

6. Exceptions to NDP-1 (reference (j)) shall not be granted to accommodate the assignment of a foreign exchange professional under the DPEP.

7. A delegation of disclosure authority letter (DDL), or equivalent written guidance, containing the information in the example in enclosure 5 shall be prepared and provided to the contact officer for each foreign national assigned to a DoD Component as a liaison officer or under a DPEP agreement.

8. A contact officer, or other experienced official, shall be designated to control the activities of foreign visitors and exchange personnel. The designated officials shall be familiar with DoD Directive 5230.11 (reference (f)), the applicable DoD Component guidelines governing the release of classified and controlled unclassified information, and the specific disclosure guidelines established in the DDL.

9. All foreign nationals, including attaches, liaison personnel, and exchange personnel who are authorized unescorted access to DoD facilities, shall be issued badges or passes that clearly identify them as foreign nationals. Decisions on issuance of badges and passes shall be made in accordance with subsection B.10. of enclosure 3.

10. The training of foreign nationals also shall be in compliance with reference (f) and DoD 5105.38-M (reference (k)).

#### **E. RESPONSIBILITIES**

1. The Under Secretary of Defense for Policy shall:

- a. Manage the Department of Defense IVP and DPEP.
- b. Manage automation support to the IVP and the DPEP through the Foreign Visits System (FVS) under DoD Instruction 5230.18 (reference (l)).
- c. Consider requests for authority to negotiate and conclude international agreements, submitted in accordance with DoD Directive 5530.3 (reference (e)), that involve the assignment of foreign exchange personnel to the DoD Components.
- d. Promulgate additional procedures, as necessary, to ensure effective implementation of this Directive.

2. The Heads of the DoD Components shall:

- a. Designate, in writing, an official to ensure effective implementation of this Directive within their Component.
- b. Promulgate written instructions, consistent with DoD Directives 5230.11, 5230.25, and 5400.7, and DoD 5200.1-R (references (f), (h), (i), and (g)), and this Directive to control access to classified and controlled unclassified information by foreign representatives who are authorized to visit or be assigned to their DoD Component.
- c. Process and record decisions on foreign visits involving access to classified and controlled unclassified information in the FVS in accordance with reference (l).
- d. Forward any inquiries concerning this Directive to the Office of the Under Secretary of Defense for Policy, Attn: Deputy Under Secretary of Defense (Security Policy).

3. The Secretaries of the Military Departments shall:

a. Establish the process at appropriate levels to approve or deny requests for visits by foreign representatives covered by this Directive to their Departments and their contractors.

b. Ensure that all agreements with foreign counterpart Military Departments involving assignments of exchange personnel are in accordance with existing laws and regulations, DoD Directive 5530.3 (reference (e)), and this Directive.

c. Direct that periodic on-site visits be made to the military organizations and facilities under their cognizance to monitor implementation of this Directive.

4. The Comptroller of the Department of Defense shall ensure that proper financial procedures affecting the DPEP are utilized.

5. The Under Secretary of Defense (Acquisition) shall promulgate procedures consistent with reference (e) and this Directive governing the negotiation and conclusion of agreements for the assignment of exchange scientific and technical personnel to the DoD Components.

6. The General Counsel of the Department of Defense shall review all international agreements submitted in accordance with reference (e) involving assignments of foreign exchange personnel to the DoD Components.

7. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall promulgate procedures consistent with reference (e) and this Directive governing the negotiation and conclusion of agreements that involve the assignment of foreign exchange personnel in DoD intelligence and intelligence-related positions.

8. The Chairman of the Joint Chiefs of Staff shall promulgate procedures consistent with reference (e) and this Directive governing visits by foreign representatives and assignments of foreign exchange personnel to the Unified and Specified Commands.

9. The Director, Defense Intelligence Agency shall:

a. Coordinate and process requests for visits by foreign representatives to the OSD, the Chairman of the Joint Chiefs of Staff, the Defense Agencies, and the DoD Field Activities, and their contractors, except for those visits approved by the Director of the National Security Agency (NSA) under paragraph 10., or the Secretary of Defense or the Deputy Secretary of Defense.

b. Administer, in coordination with the Office of the Deputy Under Secretary of Defense (Security Policy) (ODUSD(SP)), the assignment of exchange personnel to the OSD, the Chairman of the Joint Chiefs of Staff, the Defense Agencies, and the DoD Field Activities.



c. Promulgate a joint Service Foreign Attache Manual to provide Defense Attaches with standard instructions and formats governing visit requests, document requests, liaison officer certifications, and the processing of exchange personnel. The Manual shall be coordinated with the Military Departments, ODUSD(SP), and the Chairman of the Joint Chiefs of Staff before publication.

10. The Director, NSA, shall establish, control, and manage a system for administering visits and assignments of foreign representatives to the NSA and its contractors consistent with the policies established in this Directive. Such visits and assignments are not required to be processed through the DIA or in the automated FVS system described in enclosure 3.

**F. EFFECTIVE DATE AND IMPLEMENTATION**

This Directive is effective immediately. Forward two copies of implementing documents to the Under Secretary of Defense for Policy within 120 days.



Donald J. Atwood  
Deputy Secretary of Defense

**Enclosures - 6**

1. References
2. Definitions
3. IVP
4. DPEP
5. Sample DDL for Foreign Visitors and Exchange Personnel
6. Sample Certification of Conditions and Responsibilities

REFERENCES, continued

- (e) DoD Directive 5530.3 "International Agreements," June 11, 1987
- (f) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984
- (g) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
- (h) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
- (i) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
- (j) National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (short title: National Disclosure Policy (NDP-1)), October 1, 1988<sup>1</sup>
- (k) DoD 5105.38-M, "Security Assistance Management Manual," October 1988, authorized by DoD Directive 5105.38, August 10, 1978
- (l) DoD Instruction 5230.18, "The DoD Foreign Disclosure and Technical Information System (FORDTIS)," November 6, 1984
- (m) Executive Order 12356, "National Security Information," April 2, 1982
- (n) Section 1324b of title 8, United States Code, "The Immigration Reform and Control Act (IRCA)"
- (o) DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982
- (p) DoD Instruction C-5220.29, "Implementation of the North Atlantic Treaty Organization Industrial Security Procedures (U)," December 15, 1982
- (q) DoD Directive 5200.12, "Conduct of Classified Meetings," May 16, 1988
- (r) Joint Travel Regulations, Volume 2, "Department of Defense Civilian Personnel," current edition

---

<sup>1</sup> Provided to designated disclosure authorities on a need-to-know basis from the Office of the Director for International Security Programs, Office of the Deputy Under Secretary of Defense (Security Policy) (ODUSD(SP)).

## DEFINITIONS

1. Attache. A diplomatic official or military officer attached to an embassy or legation, especially in a technical capacity.
2. Certification. Formal recognition by a DoD Component of a working relationship with a representative of a foreign government (i.e., a Liaison Officer) for specified purposes and on a recurring basis over an agreed period of time.
3. Classified Military Information. Information originated by or for the Department of Defense or its Agencies or under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL as described in E. O. 12356 (reference (m)). Classified military information may be in oral, visual, or material form. DoD Directive 5230.11 (reference (f)) further defines the eight categories into which classified military information has been subdivided.
4. Contact Officer. A DoD official designated in writing to oversee and control all contacts, requests for information, consultations, and other activities of foreign representatives who are assigned to, or are visiting, a DoD Component or subordinate organization. In the case of personnel exchange programs, the host supervisor may be the contact officer.
5. Controlled Unclassified Information. Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes U.S. information that is determined to be exempt from public disclosure in accordance with DoD Directives 5230.25 and 5400.7 (references (h) and (i)) or that is subject to export controls in accordance with the ITAR (reference (b)) or the EAR (reference (c)).
6. Delegation of Disclosure Authority Letter (DDL). A letter issued by the appropriate designated disclosure authority describing classification levels, categories, scope, and limitations of information under a DoD Component's disclosure jurisdiction that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate disclosure authorities.
7. Designated Disclosure Authority. An official, designated by the Head of a DoD Component or by that DoD Component's Principle Disclosure Authority, who has been delegated disclosure authority in accordance with reference (f), to control disclosures of classified military information at subordinate commands or staff elements.
8. Executive Agent. The office or organization designated to negotiate and sign agreements establishing personnel exchange programs.

9. **Foreign Exchange Personnel.** Military or civilian officials of a foreign defense establishment (i.e., a DoD equivalent) who are assigned to a DoD Component in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DoD Component.
10. **Foreign Interest.** Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized under the laws of any country other than the United States or its possessions; and any foreign national.
11. **Foreign National.** A person who is not a citizen or national of the United States.
12. **Foreign Representative.** Any foreign interest or representative of a foreign interest.
13. **Intending Citizen.** Any foreign national who falls into one of the four categories under the Immigration Reform and Control Act of 1986 (reference (n)) (formerly "immigrant alien").
14. **Liaison Officer.** A foreign government official, either a military or civilian employee, who is certified by his or her government to act as a representative of that government to a DoD Component in connection with bilateral or multinational programs or projects.
15. **Meeting.** Any conference, seminar, symposium, exhibit, convention, training course, or other gathering during which classified or controlled unclassified information is disclosed.
16. **Representative of a Foreign Interest.** A citizen or national of the United States, or an intending citizen to the United States, who is acting as a representative of a foreign interest.
17. **Security Assurance.** The written confirmation, requested by and exchanged between governments, of the security clearance level or eligibility for clearance of their national contractors and citizens. It also includes a statement by a responsible official of a foreign government or international organization that the original recipient of U.S. classified military information possesses the requisite security clearance. It also indicates that the original recipient is approved by his or her government for access to information of the security classification involved and that the recipient government will comply with security requirements specified by the United States. In the case of industrial facilities, the security assurance should include a statement concerning the level of storage capability.

18. **Training.** Formal or informal instruction of foreign nationals in the United States or overseas by:

- a. Officers or employees of the United States, contract technicians, or contractors (including instruction at civilian institutions); or
- b. Correspondence courses; technical, educational, or information publications and media of all kinds; training aid; orientation; training exercise; and military advice to foreign military units and forces (including their military and civilian personnel).

19. **Visit Authorization.** There are three types of visit authorizations:

- a. A one-time visit authorization permits contact by a foreign representative with a DoD Component or DoD contractor facility for a single short-term occasion (normally less than 30 days) for a specified purpose.

- b. A recurring visit authorization permits intermittent visits by a foreign representative to a DoD Component or DoD contractor facility over a specified period of time for a Government-approved license, contract or agreement, or other program when the information to be released has been defined and approved for release in advance by the U.S. Government.

- c. An extended visit authorization permits a single visit by a foreign national for an extended period of time. Extended visit authorizations are to be used when a foreign national is required to be in continuous contact with a DoD Component or a DoD contractor facility beyond 30 days for one of the following situations:

- (1) A foreign government contract or joint program (e.g., joint venture, representative to a joint or multinational program, etc.);
- (2) Participation in an exchange program under the DPEP;
- (3) Training, except for those individuals on invitational travel orders; or
- (4) Liaison officers to a DoD Component(s).

## IVP

### A. GENERAL

1. Control of Visitors. Visits by foreign representatives to DoD Components and DoD contractor facilities shall be controlled to ensure that the visitors receive access to only that classified and controlled unclassified information authorized for disclosure to their government by a disclosure official designated in accordance with DoD Directive 5230.11 (reference (f)).

2. International Visits Program (IVP). The IVP is established to ensure that classified and controlled unclassified information to be disclosed to foreign representatives visiting DoD Components or DoD contractor facilities has been properly authorized for disclosure to their governments, that the requesting foreign government provides a security assurance on the visitors and their firms, if applicable, and to facilitate administrative arrangements for the visit.

3. Security Assurance. Classified information shall not be disclosed to a foreign representative unless the appropriate designated disclosure authority has received a security assurance from the foreign government being represented. Classified documentary information may not be transferred to a foreign national unless the security assurance specifically states that the individual may assume custody on behalf of the foreign government. A receipt must be obtained for classified information provided to foreign representatives, regardless of its classification level.

4. Foreign Visits System (FVS). Requests for visits submitted by foreign governments shall be submitted and processed using the FVS. Requests for visits by governments that do not participate in the FVS shall be submitted directly to the applicable Military Department or the Defense Intelligence Agency (DIA), which shall enter and process the request in the FVS.

### B. PROCEDURES

1. Recurring Visit Authorizations. Recurring visit authorizations shall be established to support intermittent, recurring visits associated with approved programs, such as agreements, contracts, or licenses. Authorizations shall be valid for the duration of the program, subject to annual review and revalidation.

2. Extended Visit Authorizations. Extended visit authorizations shall be used in circumstances described in paragraph 19.c. of enclosure 2. They may be used also for the assignment of a foreign contractor's employees if the foreign contractor is under contract to the DoD Component, and performance on the contract requires assignment of the employees to the DoD Component. Authorization shall be valid for the duration of the program, assignment, training, or certification, subject to annual review and revalidation.

3. Hosted Visit. Visits by foreign representatives at the invitation of DoD officials do not normally require the submission of a complete visit request by the visitors since designated disclosure officials should have authorized disclosures of information prior to the invitation being extended. To facilitate arrangements for these visits, DoD officials who extend such invitations shall notify their designated visitor control office of the invitation. They also should advise the invitees that security assurances must be submitted through their embassy before the visit, using the prescribed visit request format for this purpose referenced in paragraph E.9.c. of the basic document, above.

4. Visits by Foreign National Employees of U.S. Defense Contractors. Visits by such employees on official business to DoD Components or to other DoD contractor facilities do not require the submission of a visit request through foreign government channels. The requests shall be processed in compliance with DoD 5220.22-M (reference (d)). Access to export-controlled technical data by foreign national employees of U.S. contractors is authorized in accordance with an export license or by other written U.S. Government authorization that is obtained by the employing contractor. When these employees visit another contractor facility or a DoD Component, the employing facility should provide a copy of the export license or other written authorization to the designated disclosure authority or security office, as applicable, at the facility to be visited.

5. Visits by Representatives of the North Atlantic Treaty Organization (NATO)

a. One-time or recurring visits by representatives of NATO Commands or Agencies, or the NATO International Staff, that involve access to NATO classified information, shall be processed under United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN) Instruction 1-69, attachment 1, section III., paragraph 40 (enclosure 2 of DoD Directive 5100.55 (reference (o))). Recurring visits related to NATO Production and Logistics Organization or NATO Industrial Advisory Group activities shall be processed under USSAN Instruction 1-70, section VI (enclosure to DoD Instruction C-5220.29 (reference (p))).

b. Visits by representatives of a NATO Command or Agency or the NATO International Staff, including U.S. citizens assigned to NATO positions that involve access to U.S. classified information, shall be processed in accordance with the requirements of this Directive.

6. Visits for Foreign Participation in U.S. Procurement-Related Meetings Potential foreign attendance must be assumed when planning for meetings that may lead to contract opportunities for nations with which the United States has reciprocal procurement agreements. Security requirements for classified meetings shall be in accordance with DoD Directive 5200.12 and DoD 5200.1-R (references (q) and (g)). The following procedures also apply:

a. The DoD Components should determine the extent to which classified information may be involved throughout the life cycle of a program before the

announcement of a procurement action. Decisions on disclosures of classified information shall be in accordance with DoD Directive 5230.11 (reference (f)). The extent of foreign attendance at meetings related to the announced procurement action will be contingent upon the disclosure decision. If attendance by foreign representatives is permitted, any classified information to be disclosed must be at a level authorized for release to all foreign representatives that are present.

b. The Head of the DoD Component conducting the meeting, or a senior designee, shall approve any denials of a specific appeal for attendance at such meetings by a foreign government with which the Department of Defense has a reciprocal procurement agreement.

7. The DoD Components Supported by the DIA shall:

a. Obtain a disclosure authorization from the originating department or agency for the disclosure of any classified or controlled unclassified information that is not under the DoD Component's disclosure jurisdiction. This shall be done before notifying the DIA of the acceptance of a visit by foreign representatives that will involve access to such information.

b. Notify the DIA, ATTN: COS-4, when they extend invitations to foreign representatives to visit their organization.

8. DoD-authorized Visits to DoD Contractor Facilities. DoD-authorized visits of foreign representatives to DoD contractor facilities may constitute an exemption to the licensing requirements of the ITAR (reference (b)). DoD-authorized visits shall not be used to circumvent the licensing requirements of the ITAR. Therefore, DoD Components shall:

a. Approve the request for a visit and provide disclosure guidance if it is in support of an actual or planned U.S. Government program; or

b. If the proposed visit is not in support of a U.S. Government program, notify the requestor and applicable DoD contractor that arrangements for the visit may be made between the requestor and the DoD contractor, provided the DoD contractor has or obtains an export license for any technical data that may be disclosed and the necessary security assurance has been provided; or,

c. Deny the request for the visit if it is determined that the information associated with the proposed visit cannot be authorized for disclosure, and notify the requestor and the applicable DoD contractor of the decision.

9. Liaison Officers. Certification of a foreign government liaison officer does not bestow diplomatic or other special privileges, even though certified liaison officers who



also have attache status may have diplomatic accreditation by the Department of State. Liaison officers' activities shall be limited to the representational responsibilities of their government described in the certification. Liaison officers shall not perform duties that are reserved by law or regulation to an officer or employee of the U.S. Government. Liaison officers may assume custody of releasable documentary information when authorized in writing by their government. When operational requirements so dictate, strict reciprocity is not required for liaison officer assignments. The DoD certification shall not be used to assign foreign nationals to U.S. defense contractor facilities. The U.S. defense contractors must obtain an export license for such assignments and comply with Chapter 10 of DoD 5220.22-M (reference (d)). The following information shall be provided by foreign governments with their request for DoD certification of liaison officers:

- a. A statement by the sponsoring government that the proposed liaison officer is an officially sponsored representative of that government.
- b. Documentation describing the legal status of the proposed liaison officer (including any privileges and immunities to which the liaison officer is entitled) and sponsoring government responsibilities.
- c. A statement by the sponsoring government that the proposed liaison officer is authorized by the sponsoring government to conduct business with the Department of Defense for purposes that must be specified, citing related agreements, contracts, or other arrangements.
- d. An assurance by the sponsoring government that the proposed liaison officer holds a specified level of security clearance.
- e. A statement by the sponsoring government on whether the proposed liaison officer may assume custody of documentary information on behalf of the sponsoring government.
- f. An assurance that the sponsoring government will be responsible for any U.S. classified or controlled unclassified information provided to the proposed liaison officer.

10. Access to DoD Facilities. Foreign nationals may not have uncontrolled access to DoD facilities. Representatives of allied and friendly countries, usually attaches and liaison officers, may be authorized unescorted access to DoD facilities when all of the following conditions are met:

- a. The foreign government concerned extends commensurate reciprocal privileges to U.S. Defense personnel.

- b. The foreign national is sponsored by his or her government, the need for frequent access is justified, and the required security assurance is provided.
- c. Security measures are in place to control access to information and sensitive areas within the DoD facility.
- d. Access is required for official purposes on a frequent basis (i.e., more than once per week).
- e. A badge or pass is issued that identifies the bearer as a foreign national and that is valid for a specific facility during normal duty hours.
- f. The badge or pass is displayed on the outer clothing so that it is clearly visible.
- g. The request for issuance of the badge or pass must be in writing and describe how paragraph B.10.a. through f., above, will be met.

## **DPEP**

### **A. GENERAL**

1. **Background.** Since World War II, the Military Services and counterpart Services of friendly foreign military forces have entered into agreements establishing military personnel exchange programs. In accordance with these agreements, each party provides, on a reciprocal basis, assignments to established manpower positions within its force structure for military personnel of the other party. Similar agreements have been concluded for the exchange of civilian personnel in particular fields of expertise, such as scientists, engineers, and intelligence analysts. These personnel exchange programs are designed to foster mutual understanding between the Military Services of each party by providing exchange personnel familiarity with the organization, administration, and operations of the other Service. All such personnel exchange programs established by the DoD Components constitute the DPEP.

2. **Scope.** The DPEP includes all programs that involve the assignment of foreign personnel to positions with the DoD Components in exchange for the assignment of DoD personnel to positions with foreign government defense establishments, such as personnel exchanges involving the assignment of:

- a. Military or civilian personnel to positions with the Military Departments.
- b. Specialist personnel to administrative and planning positions within the OSD.
- c. Scientists and engineers to DoD Research, Development, Test, and Evaluation facilities.
- d. Intelligence analysts within the DoD intelligence community.
- e. Finance and accounting analysts within the Defense Finance and Accounting Service.

3. **Restrictions.** Assignment of foreign personnel under the DPEP shall not be used for training or instead of, or in combination with, liaison officer certification.

### **B. PROCEDURES**

1. **Status of Personnel.** Personnel assigned to DPEP positions shall be military or civilian employees of the participating DoD Component and the foreign government defense establishment.

2. **Purpose.** The DPEP agreements may be negotiated to foster better understanding on the part of the participants and their governments of the organization and

management of defense programs and operations while using the specified expertise of the participating exchange personnel. The criteria in subsection B.8. of this enclosure, below, shall be considered before making commitments for the negotiation of a DPEP agreement.

3. **Reciprocity.** The DPEP agreements shall provide for the reciprocal assignment of DoD personnel to substantially equivalent positions within the defense establishment of the other participating government.

4. **Limitations.** The DPEP may not be used as a mechanism for exchanging technical data or other controlled information between the governments or for training of foreign nationals. Information exchanges shall be governed by an appropriate agreement (e.g., cooperative research and development or data exchange agreement); training of foreign nationals shall be in accordance with DoD 5105.38-M (reference (k)).

5. **Executive Agents.** The DoD officials who are responsible for authorizing the negotiation of personnel exchange agreements may appoint an executive agent to negotiate and administer a program for a specific country or countries.

6. **Restrictions on Exchange Personnel**

a. Foreign exchange personnel shall not act in the dual capacity as a DPEP participant and as a representative of their government while assigned to a DoD Component (e.g., a DPEP participant may not act as a liaison officer).

b. Foreign exchange personnel shall not serve as a conduit between the Department of Defense and their government for requests and transmission of classified and controlled unclassified information.

c. Foreign exchange personnel may not be assigned to command or other positions that would require them to exercise responsibilities that are reserved by law or regulation to an officer or employee of the U.S. Government or that would afford them access to information that is not authorized for release to their government.

d. Foreign exchange personnel shall not be assigned to DoD contractor facilities.

7. **Security Requirements**

a. Foreign exchange personnel shall not have access to restricted areas or to the following types of information:

(1) **RESTRICTED DATA and FORMERLY RESTRICTED DATA.**

(2) Information systems security information.

(3) Classified or controlled unclassified information provided by another government, unless access is approved in writing by the originating government.

(4) Compartmented information, unless authorized by a separate government-to-government agreement.

(5) Information bearing a special handling notice that restricts access, except when authorized by the originator.

(6) Any U.S. classified information that has not been authorized previously for release to the exchange professional's government by the responsible designated disclosure authority of the originating Department or Agency.

b. Exchange personnel may not be given security responsibilities (e.g., escort responsibility, document custodian, security checks, etc.).

c. Disclosure guidance, in the form of a DDL or equivalent document, shall be established for each exchange position. The DDL shall be prepared by the host supervisor, in collaboration with the DoD Component disclosure officials, and shall accompany the request to establish a DPEP position. The Deputy Under Secretary of Defense (Security Policy) will approve the DDL for the OSD, the Chairman of the Joint Chiefs of Staff, and the Defense Agency positions. The DDL for the Military Department positions shall be approved by the designated disclosure authority of the appropriate Military Department. The information in enclosure 5 must be in the DDL.

d. Foreign exchange personnel shall not have custody of classified or controlled unclassified information. They may have access to the information during normal duty hours at the place of assignment when access is necessary to perform the functions in their position description, if the information has been properly authorized for disclosure. They may not have unsupervised access to libraries or document catalogues unless the information therein is releasable to the public.

8. DPEP Criteria. The DoD Components shall consider the following criteria before establishing a DPEP position and shall discuss them in their requests for authority to negotiate an exchange agreement:

a. Likely political or military advantage to be gained.

b. Ability to adequately use a foreign exchange person in the organization considering the policy and access limitations and security requirements described in this enclosure.

- c. Financial costs to the U.S. Government.
- d. Other military arrangements with the country and the results of those arrangements.
- e. Reciprocity, particularly the ability of the DoD Component to assign a person within the defense establishment of the other country in a similar capacity.

9. Authorized Billets. Foreign exchange personnel shall serve in authorized personnel billets or in authorized overstrength or excess positions. Exceptions to this policy may be authorized by the Head of the concerned DoD Component if the assignment will result in significant military or political benefits to the Department of Defense.

10. Position Description. A position description shall be prepared for each exchange position. The position description shall contain as a minimum:

- a. The title of the position.
- b. The position location.
- c. Qualification and skills required.
- d. Description of specific duties of the position.
- e. Security clearance level required.

11. Content of DPEP Agreement. DPEP agreements shall cover the following issues:

- a. Type of exchange positions to be established (e.g., scientist and engineer, financial management).
- b. Length of tour.
- c. Financial responsibilities (e.g., travel, salary, etc.) and use of facilities.
- d. Entitlements (e.g., commissary privileges, medical care, etc.).
- e. Liabilities and claims.
- f. Status of assigned personnel, to include privileges and exemptions.
- g. Security.

h. **Disciplinary matters.**

i. **Administrative matters and oversight responsibilities (e.g., leave, dress, reviews, and performance reports).**

12. **Administrative and Operational Control.** Foreign exchange personnel shall remain under the administrative control (e.g., pay, ratings, disciplinary actions) of their parent governments. They shall be under the operational control of the host DoD Component to which they are assigned. They may participate in the functions of the host DoD Component consistent with security considerations and the limitations described in this enclosure.

13. **Financial Responsibilities**

a. The costs of participation in the DPEP shall be borne, in accordance with applicable laws and regulations, by either the participant's parent organization or by the participant, except that travel and per diem costs for travel performed in connection with assigned duties within the host country shall be paid by the organization requesting or directing such travel.

b. Costs to be borne by the Department of Defense for its personnel shall only include salary, and, in accordance with the DoD JTR, volume 2 (reference (r)), either permanent change of station (PCS) entitlements (for the employee and his or her dependents) or long-term temporary duty entitlements. An employee of the Department of Defense that performs a PCS shall agree in writing to complete the entire period of the assignment or 1 year, whichever is shorter, unless separated or reassigned at the request of the Department of Defense.

14. **Supervisor Responsibilities.** The DoD official designated to supervise a foreign exchange person shall:

a. Ensure that the person understands the duties to be performed in the position to which he or she is assigned.

b. Ensure that the person is provided access only to that classified and controlled unclassified information necessary to fulfill the duties of the position description as described in the DDL, or as otherwise authorized in writing by the originator.

c. Ensure that coworkers are informed of the limitations on access to information by the exchange person and their responsibilities in dealing with the individual.

d. Inform the person of his or her obligations, rights, and responsibilities.

**15. Identification**

a. **Dress.** Foreign exchange personnel shall wear their military uniform, if applicable, and wear in clear view a DoD building or installation pass or badge that identifies them as foreign nationals.

b. **Status.** Any other identification issued to foreign exchange personnel by the host DoD Component shall clearly identify the person's status as a foreign exchange person.

**16. Certification of Conditions and Responsibilities**

a. Foreign exchange personnel must sign a certification similar to the sample in enclosure 6 before being assigned to the host DoD Component.

b. Foreign exchange personnel assigned to positions that might provide access to technical data also must sign a certification governing the rights of the individual and the Department of Defense on inventions and rights in property.



**SAMPLE DDL**  
**FOREIGN VISITORS AND EXCHANGE PERSONNEL**

The following DDL format should be used by DoD Components: (While all elements identified should be provided in the general order shown, information should be presented in the clearest and easiest-to-use manner.)

**TITLE:**

**DATE:**

1. **CLASSIFICATION:** Identify highest classification of information to be disclosed.
2. **DISCLOSURE METHODS:** E.g., oral, visual, or documentary. If documentary access is permitted, control procedures must be described in item 7., below.
3. **CATEGORIES PERMITTED:** Specify National Disclosure Policy categories to be disclosed.
4. **SCOPE:** Specify who is authorized to release material or information, and to whom disclosure is authorized.
5. **AUTHORIZED FOR RELEASE AND/OR DISCLOSURE:** Describe material, information, and documents to which access can be permitted. If access is permitted to information described in paragraph B.7.a. of enclosure 4, the specific agreement or other written authorization on which access is based must be cited.
6. **NOT AUTHORIZED FOR RELEASE AND/OR DISCLOSURE:** Describe material, information, and documents, or portions thereof, to which access is not permitted.
7. **PROCEDURES:** Specify review and release procedures for information that is not covered by the DDL, and describe controls and special security procedures (e.g., badges, briefings) established to limit access to information and controlled areas.
8. **REDELEGATION:** Specify the extent of redelegation of authority (if any) permitted to subordinate activities.

**SAMPLE CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES**

I understand and acknowledge that I have been accepted for assignment to (name and location of organization to which assigned) as agreed between the (name of the country's defense establishment) and the United States Department of Defense. I further understand and acknowledge that I shall comply with the following conditions and responsibilities:

a. The purpose of the assignment is to gain knowledge of the organization, management, and operation of the host defense establishment. There shall be no access to technical data or other information except that which is required to perform the duties of the position to which I am assigned.

b. I shall perform only functions as described in the Position Description for my work assignment and shall not act in any other capacity for my government.

c. Access to information shall be limited to that information determined by my designated host supervisor to be necessary to fulfill the functions described in the Position Description for my work assignment.

d. All information to which I may have access during this assignment shall be treated as information provided to my government in confidence and shall not be further released or disclosed by me to any other person, firm, organization, or government without the prior written authorization of the host government.

e. I shall not be appointed to a position that shall require me to exercise command or supervision over host government employees.

f. I have been briefed on, understand, and shall comply with all applicable security regulations of the host government.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Typed Name)

\_\_\_\_\_  
(Grade and/or Title)

\_\_\_\_\_  
(Date)